Dyachkov V. N.
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Kovaleva Aleksandra Georgievna

THREATS TO THE INFORMATION SECURITY OF ORDINARY USERS' ELECTRONIC DEVICES

Abstract. *The article examines possible threats to the information security of ordinary PC users. Since 2018, the damage from information crimes has amounted to $ 1 trillion. The problem is the inexperience of users in storing their important data on the PC. The purpose of this study is to create an algorithm and rules for the security of the user's system. This paper gives recommendations to improve the information literacy of users.*

Keywords: *Information security, antivirus, data security, data theft, brute force, cryptography, pentest, UrFU.*

Дьячков В. Н.
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ УСТРОЙСТВ ОБЫЧНЫХ ПОЛЬЗОВАТЕЛЕЙ

Аннотация. *Статья рассматривает возможные угрозы информационной безопасности обычных пользователей ПК. С 2018 года ущерб от информационных преступлений составил 1 триллион долларов. Проблема*

состоит в неопытности пользователей в хранении своих важных данных на ПК. Цель данного исследования – создать алгоритм и правила для безопасности системы пользователя. Результатом написания статья является создание таблицы для повышения информационной грамотности пользователей.

Ключевые слова: *информационная безопасность, антивирус, защищенность данных, кража данных, брутфорс, криптография, пентест, УрФУ.*

Introduction

At the moment a large number of people have switched to remote work. This means that the percentage of electronic devices use is also increasing. Devices like smartphones, PCs, laptops have already become common and everyone knows them. But few people have ever thought about the organization of information protection on their devices. This problem may reach every person, every user. The total damage from such attacks increased by about $ 423 billion between 2018 and 2020 (according to McAffee).

The conducted research is aimed at creating basic knowledge of information literacy among ordinary users of electronic devices, in order to reduce the global damage from information attacks, make it more difficult for an attacker to enter the system, and in the case of an inexperienced attacker, protect the system from data theft completely.

From password to pA4s2w-O#r5D3»

The main problem of modern users is weak passwords to their accounts, systems, and sometimes encrypted storage. A vulnerability in the passwords of the users due to their simplicity. The password «password» is used by more than 800 thousand people. The use of passwords should be reasonable and difficult to pick up.

Attackers find the correct password combination using brute force. Brute force – performing a power search of data in order to obtain the correct combination. A full search of possible passwords is performed using dictionaries. For example, a bunch of 4 NVIDIA GTX 1080ti graphics cards perform a search of 18 billion SHA256 hashes

per second. So, for a hash with an entropy of less than 40 bits, going through all the passwords will take about a minute 0.

The user needs to create a complicated password with the following recommendations:

1) Do not use simple passwords (password, 12345678, qwerty, e. t. c);
2) Change the case of letters in the password (pAsSWoRD);
3) Use special characters (#, -, e. t. c);
4) Do not use your login as a password;
5) Use numbers in combination with letters;
6) Do not use the date of birth in the password;
7) Do not make the password too short;
8) Do not use the same password everywhere.

These recommendations make it more difficult to get into your system with the help of password selection, and increase the level of security of your accounts. According to the Kaspersky Lab website, the pA4s2w-O#r5D3 password time is coming (Figure 1).

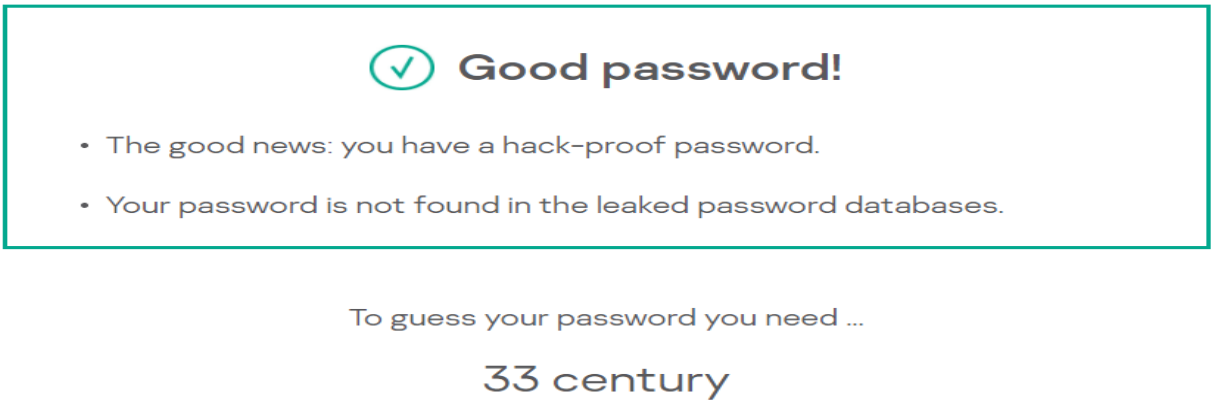

Figure 6 - Time required to guess a password

Protection and encryption of important data

Many users store important data in the system in folders, this is a big threat to the user. If a malicious program gets on the user's device, these files will be transferred to the attacker first. Because they are in the public domain on the system and most

often are not password protected. Important files may include various user passwords, information, copies of documents, and other important private information. Such information is of the greatest interest to the attacker. Protection against such an attack can be provided by the presence of an encrypted cryptographic partition on the device. On Windows, this can be implemented using «veracrypt», on Linux, it is performed using the «CryptSetup» utility.

A cryptographic file is created using the command: **dd if=/dev/zero of=~crypto.file bs=1M count=30** to create a cryptographic partition. As a result of running this program, a crypto file with a size of 30 megabytes is obtained, the size of this file can be changed by modifing the parameter «count=...». On the next step the encrypted partition is formatted. The command **cryptsetup –y –v luksFormat /*directory*/~crypto.file** is used. The system asks for the password of the crypto file in the process of executing the command. The next step is to create a virtual device to store the needed encrypted files. This step is performed using the command: **cryptsetup luksOpen /*directory*/~crypto.file partname**. Next, the file system is created in ext4 format, in the /partname section, this action is performed using the command: **mkfs.ext4 –j /*directory*/partname**. Then comes the stage of connection of the encrypted partition using the command: **mount /*directory*/partname /*directory of crypted directory***.

The result of these actions is an encrypted area in the directory that was specified last in the "mount" command. This partition becomes a normal folder, but the data contained in it is encrypted after the file is unmounted. Unmounting is performed by the following set of commands:

umount /*directory of crypted directory*

cryptsetup remove partname.

As a result of executing the commands, the encrypted area becomes the «~crypto.file» file. And it can only be viewed with the password and the necessary commands. It is necessary to write commands to open the cryptographic partition and connect it to restore the access:

cryptsetup luksOpen /*directory*/~crypto.file partname

mount /*directory*/partname /*directory of crypted directory*.

This system allows puting important files in it for the user and encrypt them after closing the section. In case of penetration into the system, the attacker will not be able to get the data that is stored in this file. Moreover, to ensure the security of valuable information, it can be stored on a separate external media and connected to it if necessary to save data or view it. Compliance with these conditions allows protecting data in the event of an intruder entering the system. Even if the penetration is successful, all important data will be stored in an encrypted area or on a separate data carrier.

Antivirus is our everything

An important part of device security is the presence of an antivirus system. If a threat is detected the program isolates the malware. Thus, ensuring the safety of the device. AV test provides ratings of antiviruses based on their effectiveness according to 3 criteria 0.

The selection is carried out according to 3 criteria, in each of which the program is able to score up to 6 points. The first and most important factor is Protection, this parameter determines which malware database the antivirus program contains to detect them. Next is the performance parameter, which is responsible for the speed of work. The last factor is Usability, a parameter that is responsible for usability (Table 1).

Table 1 - The results of testing antivirus software

Producer	Protection	Perfomance	Usability
AhnLab V3 Internet Security 9.0	6	6	6
Avast Free AntiVirus 20.7 & 20.8	6	5.5	6
AVG Internet Security 20.7 & 20.8	6	5.5	6
Avira Antivirus Pro 15.0	5.5	6	6
Bitdefender Internet Security 25.0	6	6	5.5
BullGuard Internet Security 20.0 & 21.0	6	6	6
BlackBerry Cylance Smart Antivirus 2.0	2.5	6	4
ESET Internet Security 13.2	6	5.5	6
F-Secure SAFE 17	6	6	6
GData Internet Security 25.5	6	5.5	6
K7 Security Total Security 16.0	6	6	5.5

Kaspersky Internet Security 20.0 & 21.0	6	6	6
Malwarebytes Premium 4.2.0 & 4.2.1	6	6	5
McAfee Total Protection 23.03 & 23.04	6	6	6
Microsoft Defender 4.18	6	6	6
eScan Internet Security Suite 14.0	6	6	5
Northguard Security 20.0	6	6	6
NortonLifeLock Norton 360 22.20	6	6	6
PC Matic 3.0	4	6	5
Total AV 5.8	5.5	6	6
Trend Micro Internet Security 17.0	6	6	6
Vipre AdvancedSecurity 11.0	6	6	6

In order to secure the system an antivirus program that scores at least 5 points for each column should be chosen. The presence of such a program increases the level of security of the data and system. These programs are to recognize a malicious program that is hidden behind a normal program. The antivirus program allows running suspicious files in the "sandbox", where they are not able to harm the system. A full scan of the system should be done permanently to provide high level of security.

The most important condition for the security of users' devices is to be careful, not to trust unknown sources and unlicensed software. The most important recommendations are collected in Figure 2.

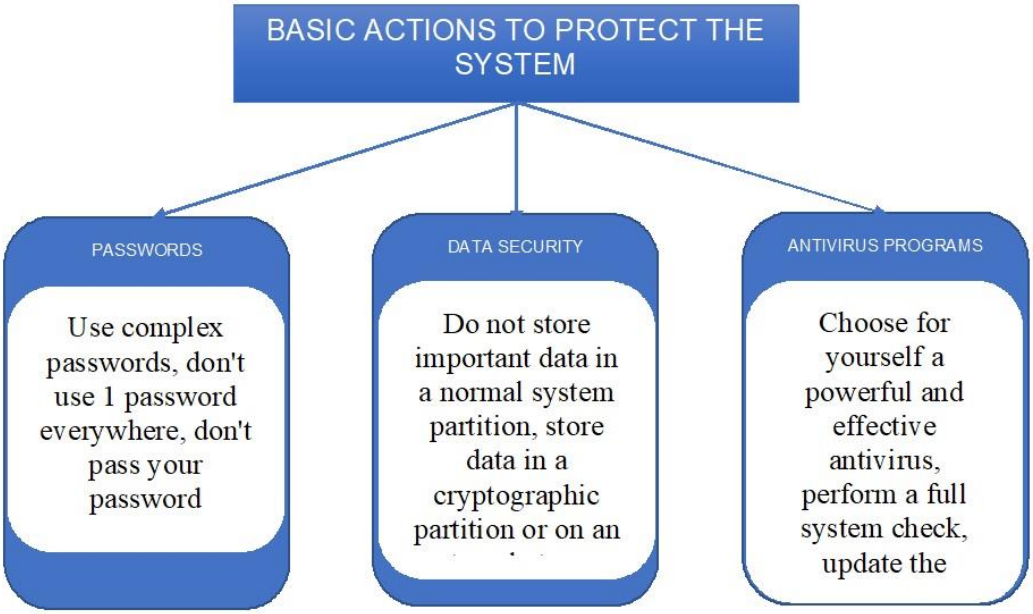

Figure 2 - Guide to information security

This paper studies the methods of attacking users' systems in order to steal information and provides main methods of protection. The methods significantly increase the security of users' information in the devices. Valuable information and data are more likely to be saved if users apply these methods of information protection and the amount of information attacks will be significantly reduced.

REFERENCES

1. S. Y. Enoch, Z. Huang, C. Y. Moon, D. Lee, M. K. Ahn and D. S. Kim. - HARMer: Cyber-Attacks Automation and Evaluation // IEEE Access, vol. 8, pp. 129397-129414/ Text: electronic. (Reference date 26.12.2020).

2. AV-TEST - The Independent IT-Security Institute – The best Windows antivirus software for home users – 2020. – Text: electronic. – URL: https://www.av-test.org/en/antivirus/home-windows/ (Reference date 26.12.2020).

3. James Andrew Lewis, Zhanna Malekos Smith, Eugenia Lostri. The Hidden Costs of Cyebercrime. – December 9, 2020. – Text: electronic. – URL: https://www.csis.org/analysis/hidden-costs-cybercrime (Reference date 26.12.2020).

4. Alexey Ermishin. Make passwords great again! Как победить брутфорс и оставить хакеров ни с чем. – 2018. – Text: electronic. – URL: https://www.highload.ru/moscow/2018/abstracts/3865 (Reference date 26.12.2020).